GLOBAL SOLUTION FOR CROSS-BORDER DATA TRANSFERS: MAKING THE CASE FOR CORPORATE PRIVACY RULES*

MIRIAM WUGMEISTER,** KARIN RETZER,*** CYNTHIA RICH****
MORRISON & FOERSTER LLP

I. INTRODUCTION

Technology has radically changed the manner in which information flows around the world. Global transfers of information are now a common and essential component of our daily lives. Sharing information allows businesses to provide consumers with enhanced services such as 24-hour customer hotlines as well as a greater choice of products and services at lower prices. At the same time, businesses are able to manage their operations in a more cost effective and efficient manner. Countries, in turn, benefit from increased global business investment and activity. All in all, consumers, businesses and governments receive enormous benefits from global data transfers.

Nevertheless, such transfers are becoming more difficult and costly from a business perspective as more countries adopt privacy laws that, among other things, regulate and limit cross-border transfers of personal information, including transfers to headquarters, affiliates, branch offices or subsidiaries. Typically these laws either explicitly prohibit transfers to other countries unless certain conditions are met or impose regulatory obligations on the organizations transferring the personal information. Many of these laws are enacted in response to growing public concern about the potential and actual misuse of personal information in an increasingly networked economy.

Privacy laws, however, vary dramatically from country to country. Some countries have enacted comprehensive laws while others have

---

** Miriam Wugmeister is a Partner at the law firm of Morrison & Foerster LLP. She heads the Firm's Global Privacy and Data Security Practice and is resident in the New York office of Morrison & Foerster. She can be reached at mwugmeister@mofo.com.

*** Karin Retzer is an Of Counsel at the law firm of Morrison & Foerster LLP. She leads the Firm's European Privacy and Data Security Practice and is resident in the Brussels office of Morrison & Foerster. She can be reached at kretzer@mofo.com.

**** Cynthia Rich is a Senior Policy Analyst at the law firm of Morrison & Foerster LLP. She is a key member of the Firm's Privacy and Data Security Practice and is resident in the Washington DC office of Morrison & Foerster. She can be reached at crich@mofo.com.

little or no rules in place. For those countries that do have laws in place, the standard of protection provided for in the law, its interpretation and the level of enforcement can vary significantly.

At the same time, the cross-border limitations are adversely affecting both the quality and choice of products and services that can be offered to consumers on a global basis. Consumers and employees (herein referred to as "individuals") as well as businesses are equally ill served by this patchwork arrangement of cross-border privacy protections.

As a result, greater attention is being paid to the development and use of global or enterprise-wide privacy rules ("Corporate Privacy Rules") as a way to correct the problems associated with this patchwork of cross-border privacy rules. Under Corporate Privacy Rules, businesses would establish their own set of rules for the transmission of personal information via the Internet. These rules would incorporate internationally accepted principles of fair information practices. If all affiliates are subject to the Corporate Privacy Rules, then a business could freely move information within the entire group, e.g., between headquarters, subsidiaries, branch offices and any affiliated entities.

The concept of Corporate Privacy Rules is based on the notion of accountability—that is, the organization as a whole assumes responsibility for protecting the data. Corporate Privacy Rules are not a new concept; rather, they are an extension of an approach that has worked successfully in other areas for many years (e.g., enterprise-wide policies in the field of financial reporting and determination of conflicts of interest). The challenge, however, will be to secure the necessary international acceptance and cooperation that will enable businesses to implement Corporate Privacy Rules as a global, rather than a national or regional, solution for cross-border data transfers.

Two of the major stumbling blocks to the widespread acceptance and use of Corporate Privacy Rules are concerns about the manner in which such rules can be enforced under existing laws and methods to secure the necessary cooperation among the respective enforcement authorities in the event of cross-border disputes or breaches. These stumbling blocks, however, are not insurmountable, contrary to what some in the data protection community might think. As we will explain, there are other laws such as those that pertain to unfair commercial practices which can be used to enforce Corporate Privacy Rules. Moreover, while cross-border cooperation is not easy to accomplish, it is not unprecedented. There are many areas in which government agencies around the world are already collaborating. These existing arrangements could serve as a source or model for cooperation in the privacy area.

Before addressing the issues of enforcement and cross-border cooperation, this article will provide an overview of the international privacy legislative landscape and the difficulties that arise on a practical level from both a consumer and business perspective. It will then assess the current options available for cross-border transfers, identify the advantages and disadvantages of same, and then discuss how Corporate Privacy Rules can be used to overcome the current difficulties.

II. Privacy Laws—an Overview

A. *Privacy Landscape*

More than sixty countries around the world have laws that regulate the collection, use and disclosure of personal information.[1] Typically these laws cover any personal information pertaining to individual customers, business contacts, consumers, employees and in some cases legal entities. By and large, these laws require that the collection of personal information or establishment of databases containing personal information be publicly disclosed and that these activities be registered with the government or with an independent data protection authority ("DPA"). They also require that individuals whose personal information is maintained by an organization be given notice of, and in certain circumstances the right to consent (or to withhold consent) to, the collection, use and transfer of their personal information, as well as the right to access and correct the information held about them. In addition, organizations must protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Growing concerns about data security have resulted in some countries prescribing detailed technical and organizational security measures.

The laws of some of these nations also require the permission of a DPA to "export" or transfer personal information. These DPAs may refuse permission if the data protection laws of the receiving country are not considered to be as strong as those of the home country. Failure to adhere to these rules may result in civil and/or criminal penalties for the organization concerned.

Countries or jurisdictions that now have privacy statutes include:

1. "Personal information" as used in this Article denotes any information about an identified or identifiable individual.

- **Asia**: Australia,[2] Japan,[3] Hong Kong,[4] Macau,[5] New Zealand,[6] South Korea[7] and Taiwan;[8]
- **Europe**: the 27 European Union (EU) Member States,[9] Albania,[10]

---

2. Privacy Act 1988 (amended 2006), *available as amended at* http://www.privacy.gov.au/publications/privacy88130706.pdf.

3. Kojin Joho Hogo Ho [Act on the Protection of Personal Information], Law No. 57 of 2003, *available in unofficial English translation at* http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.

4. Personal Data (Privacy) Ordinance, (1995) Cap. 486. (H.K.), *available at* http://www.pcpd.org.hk/english/ordinance/down.html.

5. Lei da Protecção de Dados Pessoais [Personal Data Protection Law], Lei No. 8/2005, No. 34 Boletim Oficial da Região Administriva Especial de Macau I Serie 868 (2005) (Mac.), *available at* http://images.io.gov.mo/bo/i/2005/34/lei-8-2005.pdf.

6. Privacy Act, 1993 S.N.Z. No. 28, *available at* http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes.

7. Act No. 5835 [Promotion of Information and Communications Network Utilization and Information Protection] (2005) (amended 2005), *available in unofficial English translation at* http://www.worldlii.org/int/other/PrivLRes/2005/2.html.

8. The Computer-Processed Personal Data Protection Law (1995), *available in unofficial English translation at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national_laws/Taiwan-CP-DPLaw.pdf.

9. The twenty-seven EU Member States and their respective data protection acts are: *Austria*—Bundesgesetz über den Schutz personenbezogener Daten [Datenschutzgesetz 2000-DSG 2000] [Federal Act Concerning the Protection of Personal Information] Bundesgesetzblatt Teil I [BGBl I] No. 165/1999 (amended 2001) (Austria), *available at* http://www.dsk.gv.at/dsg2000e.pdf; *Belgium*—La Loi Relative à la Protection des Données à Caractère Personnel [Privacy Protection in Relation to the Processing of Personal Data] (1992) (amended 1999), *available at* http://www.privacycommission.be/textes_normatifs/loi_wet_8_12_92%20.pdf *and in unofficial English translation at* http://www.law.kuleuven.ac.be/icri/publications/499Consolidated_Belgian_Privacylaw_v200310.pdf; *Bulgaria*—Personal Data Protection Act 2002, State Gazette No. 1/4.01.2002 (amended 2006), *available in unofficial English translation at* http://www.aip-bg.org/pdf/pdpa.pdf; *Cyprus*—The Processing of Personal Information (Protection of Individuals), Law 138 (I) (2001) (amended 2003), *available in English translation at* http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument; *Czech Republic*—[Personal Data Protection Act], zákon č. 101/2000, *available in unofficial English translation at* http://www.uoou.cz/index.php?l=en&m=left&mid=01:01:01&u1=&u2=&t=; *Denmark*—Act on Processing of Personal Data, Act No. 429 (2000), *unofficial English translation available at* http://www.datatilsynet.dk/attachments/20001061548/ENGELSK%20LOV.doc; *Estonia*—Isikuandmete Kaitse Seadus [Personal Data Protection Act] (2003), Riigi Teataja [RT I] 2003, 26, 158 (amended 2004), *available at* https://www.riigiteataja.ee/ert/act.jsp?id=264800 *and in unofficial English translation at* http://www.legaltext.ee/text/en/X70030.htm; *Finland*—Personuppgiftslag [Personal Data Act], 523/1999 (amended 2000), *available at* http://www.abo.fi/dc/admin/reglerlagar/L-personuppgifter.pdf *and in unofficial English translation at* http://www.tietosuoja.fi/uploads/hopxtvf.HTM; *France*—Law No. 78-17 of Jan. 6, 1978 [Data Processing, Data Files and Individual Liberties], Journal Officiel de la République Française [J.O.] [Official Gazette of France], Jan. 7, 1978 (amended 2004), *available in official English translation at* http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf; *Germany*—Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Dec. 20, 1990 BGBl. I 1990 at 2954, *available at* http://www.bfdi.bund.de/cln_030/nn_

Bosnia and Herzegovina,[11] Croatia,[12] Iceland,[13] Liechtenstein,[14]

946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct, templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf; *Greece*—Nomos (1997:2472) [Protection of Individuals with Regard to the Processing of Personal Data] (amended [year]), *available at* http://www.dpa.gr/law2472.htm, *English translation available at* http://www.dpa.gr/Documents/Eng/2472engl_all.doc; *Hungary*—1992. évi LXIII. Törvény a személyes adatok védelméröl és a közérdekü adatok nyilvánosságáról [Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest], Magyar közlöny [MK.] 1992 no. 116, *available at* http://abiweb.obh.hu/dpc/index.htm; *Ireland*—Data Protection (Amendment) Act 2003 (Act No. 6/2003), *available at* http://www.dataprotection.ie/documents/legal/act2003.pdf; *Italy*—Codice in materia di protezione dei dati personali [Italian Personal Data Protection Code], Decreto Legislativo di 30 Jun 2003 [Legislative Decree of June 30, 2003], Gazz. Uff. July 29, 2003, n. 196, *unofficial English translation available at* http://www.privacy.it/privacycodeen.html; *Latvia*—Fizisko personu datu aizsardzības likums [Personal Data Protection Law of 2000], Vēstnesis 123/124 06.04.2000, *available in unofficial English translation at* http://www.dvi.gov.lv/eng/legislation/pdp/; *Lithuania*—Asmens duomenų teisinės apsaugos istatymas [Law on Legal Protection of Personal Data] (2003) 2003 m. sausio 21 d. Nr. IX-1296 (amending the Law of the Republic of Lithuania on Legal Protection of Personal Data), *available at* http://www.ada.lt/images/cms/File/pers.data.prot.law.pdf; *Luxembourg*—Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel [Law on the Protection of Persons with Regard to the Processing of Personal Information] (2002), Mémorial Journal Officiel du Grand-Duché de Luxembourg, A-nº 91 p. 1836, *available at* http://www.legilux.public.lu/leg/a/archives/2002/0911308/0911308.pdf#page=2; *Malta*—Att dwar il-Protezzjoni u l-Privatezza tad-Data [Data Protection Act], 2001 Cap. 440. 1 (as amended), *available in unofficial English translation at* http://www.dataprotection.gov.mt/dbfile.aspx/DPA.pdf; *Netherlands*—Wet bescherming persoonsgegevens [Personal Data Protection Act] Stb. 2000, 302, *available in unofficial English translation at* http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true&theme=purple; *Poland*—Dziennik ustaw Rzeczypospolitej Polskiej [Act on the Protection of Personal Data] (1997) no. 133, item 833 (amended 2002), *available at* http://www.giodo.gov.pl/data/filemanager_en/61.pdf; *Portugal*—Lei da Protecção de Dados Pessoais [Law to Protect Personal Data] (1998), Diário da república 67/98, *available in unofficial English translation at* http://www.cnpd.pt/english/bin/legislation/Law6798EN.HTM; *Romania*—Law No. 677/2001 for the Protection of Persons Concerning the Processing of Personal Data and Free Circulation of Such Data, Monitorul Oficial 2001 no. 790, *available in unofficial English translation at* http://www.dataprotection.ro/images/PDF/Law677_en.pdf; *Slovakia*—Zbierka zákonov [Protection of Personal Data] č. 428/2002, Čiastka 167, strana 4403 (as amended), *available at* http://www.zbierka.sk/get.asp?rr=02&zz=02-z428, *unofficial English translation available at* http://www.dataprotection.gov.sk/buxusnew/docs/act_428.pdf; *Slovenia*—Zakon o varstvu osebnih podatkov [ZVOP-1] [Personal Data Protection Act] (2004), Uradni list Republike Slovenije [Official Gazette of the Republic of Slovenia], No. 86/2004 (partially annulled and corrected by the Information Commissioner Act, Uradni list Republike Slovenije, No. 113/2005), *unofficial English translation available at* http://www.ip-rs.si/index.php?id=162; *Spain*—Protección de Datos de Carácter Personal [Protection of Personal Information] B.O.E. 1999, 298 (amended 2003), *available at* http://civil.udg.es/normacivil/estatal/persona/PF/Lo15-99.htm, *unofficial English translation available at* https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf; *Sweden*—Personuppgiftslag [Personal Data Act] (Svensk författningssamling [SFS] 1998:204) (Swed.), *available in unofficial English translation at* http://www.sweden.gov.se/content/1/c6/01/

Macedonia,[15] Norway,[16] Russian Federation,[17] and Switzerland;[18]
- **Middle East/Africa**: Israel,[19] Mauritius,[20] Tunisia[21] and the U.A.E. (DIFC);[22] and

55/42/b451922d.pdf; *The United Kingdom*—Data Protection Act, 1998, c. 29 (amended 2000), *available at* http://www.opsi.gov.uk/acts/acts1998/19980029.htm.

10. Ligji 8517 of July 22, 1999 [On the Protection of Personal Data], Fletorja zyrtare Republikës të Shqipërisë, No. 23, Sep. 4, 1999, 839 (Alb.), *unofficial English translation available at* http://www.hidaa.gov.al/english/pub/l_8517.htm.

11. Law on the Protection of Personal Data, Official Gazette of Bosnia and Herzegovina 32/01, *unofficial English translation available at* http://www.privacyinternational.org/countries/bosnia/bosnia-dpa.html.

12. Law of June 12, 2003 [Act on Personal Data Protection], Narodne novine; sluzbeni list Republike Hrvatske 2003 no. 103, item 1364 (Croat.), *English translation available at* http://www.azop.hr/DOWNLOAD/2005/02/16/Croatian_Act_on_Personal_Data_Protection.pdf.

13. Act No. 77/2000 [Act on the Protection of Privacy as Regards the Processing of Personal Data] (as amended) (Ice.), *unofficial English translation available at* http://www.personuvernd.is/information-in-english/greinar//nr/438.

14. Datenschutzgesetz (DSG) [Data Protection Act], Liechtensteinisches Landesgesetzblatt [LGBI] 2002 no. 55 (Liech.), *available at* http://www.gesetze.li/get_pdf.jsp?PDF=2002055.pdf.

15. Law 12/94, Law on Personal Data Protection, Official Journal of Rep. of Macedonia 12/94, *available at* http://www.libertas-institut.com/de/MK/nationallaws/Law_on_personal_data_protection.pdf.

16. Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data, *English translation available at* http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf.

17. Federal law 152-FZ [Personal Data], Roz. gaz., Jul. 29, 2006, 4131, *available at* http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html, *unofficial English translation available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1625/Privacy_Russia_White_Paper.pdf.

18. Loi fédérale sur la protection des données [LPD] [Federal Act on Data Protection], Recueil officiel des lois fédérales, June 19, 1992, RO 235.1, *available at* http://www.admin.ch/ch/f/rs/2/235.1.fr.pdf, *unofficial English translation available at* http://www.edoeb.admin.ch/org/00828/index.html?lang=en.

19. The Protection of Privacy Law (Amendment) 5745-1985, 1011 LSI 128 (1981-82) (Isr.).

20. Act 13 of 2004 [Data Protection Act], *available at* http://www.gov.mu/portal/goc/telecomit/files/dpa04.doc.

21. Loi portant sur la Protection des Données à Caractère Personnel [Supporting Law on the Protection of Personal Data], No. 2004-63, Jul. 27, 2004 (Tunis.), *available at* http://www.jurisitetunisie.com/tunisie/codes/ce/pdmenu.html.

22. Data Protection Law 2007, DIFC Law No. 1 of 2007, *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

• **North/South America**: Argentina,[23] Canada,[24] Chile,[25] Paraguay,[26] Peru,[27] the United States,[28] and Uruguay.[29]

Moreover, many other countries are debating or considering privacy legislation, including Barbados, Bolivia, Brazil, China, Costa Rica, Ecuador, India, Jordan, Lebanon, Malaysia, Mexico, Morocco, Pakistan, Panama, Singapore, South Africa, Sri Lanka, Tanzania, Thailand, Trinidad and Tobago, Turkey, the Ukraine, and Venezuela.

B. *Local Compliance Obligations*

Europe

The twenty-seven Member States of the European Union (EU) have adopted comprehensive privacy laws based on the 1995 Data Protection Directive[30] (the "EU Directive"). The laws of the members of the European Economic Area (EEA), i.e., Iceland, Liechtenstein, and Norway, provide for very similar requirements, and the laws of neighboring countries such as Albania, Andorra, Bosnia and Herzegovina, Croatia, Macedonia, and Switzerland largely reflect the EU Directive. The Russian Federation has also recently adopted legislation that is similar to the EU Directive.

Personal information is very broadly defined as "any relating to an identified or identifiable natural person."[31] An identifiable person is

---

23. Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html.

24. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5, *available at* http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf.

25. Law 19628 [Protection of Personal Data], Diario Oficial, Aug. 28, 1999 (as amended) (Chile), *available at* http://www.sernac.cl/leyes/compendio/Leyes/Ley_19.628_sobre_Proteccion_de_la_Vida_Privada_y_Datos_Personales.pdf.

26. Ley 1969 [Private Information], Registro oficial de la República del Paraguay, Jan. 19, 2001 (as amended), *available at* http://www.informconf.com.py/informconf/site/downloads/Ley_1682.pdf.

27. Law No. 27489, Centrales Privadas de Información de Riesgo (CEPIRS) (Peru), *available at* https://www.agpd.es/upload/C.5)%20Ley%20peruana%20de%20protecci%F3n%20de%20datos.pdf.

28. 15 U.S.C. §§ 6801–6809 (2000); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-91, 110 Stat. 1936 (codified in scattered sections of 42 U.S.C.).

29. Ley 17,838 [Protection of Personal Information in Commercial Sources and Recognizing the Right of Habeas Data Action], D.O. 1, Oct/004, No. 26599 (Uru.), *available at* http://www.parlamento.gub.uy/Leyes/Ley17838.htm.

30. Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31.

31. *Id.* at 138, art. 2(a).

one who can be identified, directly or indirectly, taking account of all means that are likely to be reasonably used either by the controller or by any other person to identify the said person.[32]

According to the EU Directive, personal information can only be processed when one of the following exceptions is met: consent from the individual; contractual necessity (that is, data may be used if necessary for the performance of the contract with the individual); compliance with (local) legal obligations; or the legitimate interests of the entity collecting the personal information outweigh the privacy interests of the individual.

Asia, Americas, Middle East, and Africa

Unlike in Europe, the data privacy laws elsewhere around the world vary more widely from country to country, particularly with respect to the processing of certain types of personal information and database registration.

For example, Hong Kong, Japan, and New Zealand regulate the processing of personal information in all sectors; Australia regulates all sectors of the economy but exempts much of employee data from requirements of its Act; Taiwan and, to some extent, Korea regulate only selected sectors of the economy.[33]

In the Americas, only a few countries have adopted omnibus data protection laws. Argentina has adopted legislation that is similar to the EU Directive, but it only regulates the collection, use, and disclosure of personal information contained in databases that are shared.[34] Chile regulates the processing and use of personal information by the public and private sectors, and has specific provisions that pertain to the use of financial, commercial and banking data, as well as the use of informa-

---

32. *Id.* at 133, rec. 26.

33. *See* Personal Data (Privacy) Ordinance, (1995) Cap. 486. (H.K.), *available at* http://www.pcpd.org.hk/english/ordinance/down.html; Kojin Joho Hogo Ho [Act on the Protection of Personal Information], Law No. 57 of 2003, *unofficial English translation available at* http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf; Privacy Act, 1993 S.N.Z. No. 28, *available at* http://www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes; Privacy Act 1988, 1988 (as amended), *available at* http://www.privacy.gov.au/publications/privacy88130706.pdf; Computer-Processed Personal Data Protection Law (1995), *unofficial English translation available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national_laws/Taiwan-CP-DPLaw.pdf; Act No. 5835 [Promotion of Information and Communications Network Utilization and Information Protection] (2005) (as amended), *unofficial English translation available at* http://www.worldlii.org/int/other/PrivLRes/2005/2.html.

34. Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html.

tion by government agencies.[35] Canada regulates the collection, use, and disclosure of personal information by all private sector businesses in the course of their commercial activities, except in provinces that have enacted legislation deemed to be substantially similar to federal law.[36] Canada's federal law does not generally apply to employee information unless the business is in the telecommunications, broadcasting, inter-provincial or international transportation, aviation, banking, or nuclear energy sectors.[37]

In Africa, only Tunisia and Mauritius have adopted comprehensive privacy laws. While the Tunisian law follows the EU Directive, it imposes even stricter requirements for processing information and in particular for cross-border transfers.[38] In Mauritius, both notice and opt-in consent are required to collect, use, and transfer personal information unless the information is required for the performance of the contract.[39]

The Middle East, Israel, and the United Arab Emirates (DIFC) require DPA authorization, contractual safeguards and/or opt-in consent to process and transfer personal information outside the respective countries.[40]

C. *Rules for Cross-Border Data Transfers*

Most if not all of the countries that have enacted privacy laws have rules that regulate the transfer of personal information. Transfer covers any sharing, transmission or disclosure of, providing access to, or otherwise making available, information to third parties. Third parties include corporate affiliates as well as government authorities. Some countries do impose specific restrictions on cross-border trans-

35. Law 19628 [Protection of Personal Data], Diario Oficial, Aug. 28, 1999 (as amended) (Chile), *available at* http://www.sernac.cl/leyes/compendio/Leyes/Ley_19.628_sobre_Proteccion_de_la_Vida_Privada_y_Datos_Personales.pdf.

36. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5, *available at* http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf.

37. *Id.*

38. Loi portant sur la Protection des Données à Caractère Personnel [Supporting Law on the Protection of Personal Data], No. 2004-63, Jul. 27, 2004, at ch. 2-4, *available at* http://www.jurisitetunisie.com/tunisie/codes/ce/pdmenu.html.

39. Act 13 of 2004 [Data Protection Act] § 22, *available at* http://www.gov.mu/portal/goc/telecomit/files/dpa04.doc.

40. *See* The Protection of Privacy Law (Amendment), 5745-1985, 1011 LSI 128 (1981-82) (Isr.); Data Protection Law 2007, DIFC Law No. 1 of 2007 (U.A.E.), *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

fers; alternatively, others require the organization collecting the information to impose certain requirements on the recipient entity, such as contractual undertakings.

Countries That Restrict Cross-Border Data Transfers

European Union

The transfer of personal information to countries outside the EEA is prohibited unless the receiving countries provide an "adequate" level of protection, as determined by the European Commission or national DPAs, or the transfer satisfies one of the exceptions contained in the law. Any business operating in the EU that fails to meet these conditions may incur substantial legal liability. To date, the European Commission has deemed adequate the laws of Argentina,[41] Canada,[42] Guernsey,[43] the Isle of Man,[44] and Switzerland,[45] as well as the U.S. Safe Harbor Framework.[46]

The laws of the EU and its Member States also provide several exceptions that allow for international transfers of personal information where there has been no determination of adequacy for the receiving jurisdiction. These exceptions include situations where: (i) the individual has given his or her unambiguous consent; (ii) the transfer is necessary for the performance of the contract with the individual, or concluded in the interest of the individual; or (iii) the transfer is necessary for the defense of a legal claim.[47] EU privacy regulators do, however, interpret these exceptions narrowly.

---

41. *See* Commission Decision No. 1731/2003 of 30 June 2003, art. 1, 2003 O.J. (L 168) 5 (EC), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf.

42. *See* Commission Decision No. 2/2002 of 20 Dec. 2001, art. 1, 2002 O.J. (L 2) 13 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_002/l_00220020104en00130016.pdf.

43. *See* Commission Decision No. 821/2003 of 21 Nov. 2003, art. 1, 2003 O.J. (L 308) 27 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_308/l_30820031125en00270028.pdf.

44. *See* Commission Decision No. 411/2004 of 28 Apr. 2004, art. 1, 2004 O.J. (L 152) 48 (EC) (as corrected by Corrigendum to Commission Decision No. 411/2004, 2004 O.J. (L 208) 47), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0411R(01):EN:HTML.

45. *See* Commission Decision No. 518/2000 of 26 July 2000, art. 1, 2000 O.J. (L 215) 1 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00010003.pdf.

46. *See* Commission Decision No. 520/2000 of 26 July 2000, art. 1, 2000 O.J. (L 215) 7 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00070047.pdf.

47. Council Directive 95/46, art. 26, 1995 O.J. (L 281) 31 (EU), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

Alternatively, a business may transfer personal information to a recipient country that does not provide adequate protection if it ensures that "adequate safeguards" are in place when the information is to be transferred. Traditionally, this entails the establishment of contracts between the entity sending the data (the "exporter") and the receiving entity (the "importer"). Approval of most Member State DPAs is required if individually negotiated contacts ("ad hoc contracts") are used. Contracts that incorporate certain standard contractual clauses approved by the European Commission ("Standard Clauses")[48] do not require DPA approval.

When Standard Clauses were introduced, it was hoped that because they provided one form of contract useable in all EU Member States and required no approval by individual DPAs, they would create workable and substantially more streamlined international data transfers. Unfortunately, it appears that the drawbacks of Standard Clauses may outweigh their advantages. Besides entailing burdensome compliance requirements, Standard Clauses require that all individuals to whom the information relates be made third party beneficiaries of the agreement between the exporter and the importer, providing individuals with a direct cause of action and imposing liabilities on both the exporter and the importer. Further, an importer may generally only provide the information to third parties if those third parties are either subject to an adequacy finding, executed the Standard Clauses, or consent is obtained from each and every individual whose information will be transferred. Only in environments where the data flow is stable and fairly limited would such limitations be practical.

In addition, both ad hoc contracts and Standard Clauses can be very difficult to administer. Data flows do not follow neat or well-established paths, but travel along multiple paths through a multitude of channels, through e-mail exchange, access to databases, and intranets. Global organizations have complex organizational structures that can change frequently. Unless regularly revised—at considerable expense—

48. *See* Commission Decision No. 497/2001 of 15 June 2001, 2001 O.J. (L 181) 19 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2001/l_181/l_18120010704en00190031.pdf. The European Commission has also adopted standard contractual clauses for the transfer of personal information to third countries from a data controller to a data processor. *See* Commission Decision No. 16/2002 of 27 December 2001, 2002 O.J. (L 6) 52 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_006/l_00620020110en00520062.pdf. In 2004, the European Commission amended its 2001 Decision and added a new set of standard contractual clauses. *See* Commission Decision No. 915/2004 of 27 Dec. 2004, 2004 O.J. (L 385) 74, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00740084.pdf.

contracts will not be able to reflect the changes in usage of information in organizations, as required under the contract regime.

Argentina, Australia, Mauritius, Tunisia and the United Arab Emirates (U.A.E.)[49]

Like the EU, Argentina also prohibits transfers to countries without "adequate" data protection, but because Argentina has not issued any adequacy findings, organizations must rely on contracts or the consents of individuals. Similarly, Mauritius, Tunisia, and the U.A.E. restrict transfers to countries that do not provide "adequate protection" and require opt-in consent and/or a DPA permit or authorization. In addition, Australia permits organizations to transfer personal information to a recipient in a foreign country only if it is subject to a "substantially similar" privacy regime; however, organizations must determine for themselves what constitutes "substantially similar."

Countries that Impose Accountability Obligations

Canada & Japan[50]

In contrast, the laws in Canada and Japan do not distinguish between cross-border and domestic transfers to third parties. They apply the same rules to all third parties, regardless of their location. Third parties include affiliates, subsidiaries and parent organizations. In brief, these laws require organizations to remain accountable for protecting personal information transferred to third parties. This means, in the case of Canada, that organizations that hold personal information and transfer it to third parties must include a privacy protection clause in

49. *See* Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html; Privacy Act, 1988 (as amended) (Austl.), *available at* http://www.privacy.gov.au/publications/privacy88130706.pdf; Act 13 of 2004 [Data Protection Act], *available at* http://www.gov.mu/portal/goc/telecomit/files/dpa04.doc (Mauritius); Loi portant sur la Protection des Données à Caractère Personnel [Supporting Law on the Protection of Personal Data], No. 2004-63, Jul. 27, 2004 (Tunis.), *available at* http://www.jurisitetunisie.com/tunisie/codes/ce/pdmenu.html; Data Protection Law 2007, DIFC Law No. 1 of 2007 (U.A.E.), *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

50. *See* Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5, *available at* http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf; Kojin Joho Hogo Ho [Act on the Protection of Personal Information], Law No. 57 of 2003, *unofficial English translation available at* http://www5.cao.go.jp/seikatsu/kojin/foreign/act.pdf.

contracts to guarantee that the third party provides the same level of protection as does the organization that originally collected the personal information. In Japan, organizations must establish contracts with service providers and other third parties that contain specific data security provisions.

Countries that Impose Consent or Other Requirements

Korea & Taiwan[51]

Cross-border agreements to transfer personal information to third parties outside of Korea and Taiwan are not required; however, Korea does require opt-in consent to transfer personal information, while Taiwan requires that entities subject to the privacy law obtain a license to process and transfer personal information abroad. At present, the Taiwanese law is limited to certain private entities such as financial, securities, insurance, mass media, and telecommunications companies but there is a new privacy law pending before the Taiwanese legislature, which, if enacted, would cover companies in all industry sectors. Korea also has more than one draft privacy law pending but the leading proposal does not specify the rules for cross-border transfers; instead, it directs the government to develop a policy in the future to address this issue.

III. Assessing the Current Options for Cross-Border Transfers

Most businesses that wish to transfer personal information currently use one of three options: obtain the consent of the individual concerned; establish a contract between the entities exchanging the information; or if transferring from the EU, limit data flows to jurisdictions where there is an "adequacy" finding such as the U.S. Safe Harbor regime.[52]

---

51. *See* Act No. 5835 [Promotion of Information and Communications Network Utilization and Information Protection] (2005) (as amended) (Korea), *unofficial English translation available at* http://www.worldlii.org/int/other/PrivLRes/2005/2.html [herinafter PICNU]; The Computer-Processed Personal Data Protection Law (1995) (as amended) (Taiwan), *unofficial English translation available at* http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/national_laws/Taiwan-CP-DPLaw.pdf.

52. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 56,534 (Sept. 19, 2000); Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,666 (Jul. 24, 2000). *See also* Safe Harbor, http://www.export.gov/safeharbor/doc_safeharbor_index.asp (last visited May 13, 2007).

In some situations, however, organizations may be unable to rely on the use of the three options above to make their international data transfers legal. For example, many banks function internationally through branches rather than through separate legal entities; therefore, contracts generally cannot be used when the same legal entity would be on both sides of the contract. Likewise, only organizations subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation are currently eligible to join the Safe Harbor, thereby excluding participation by financial services institutions and telecommunications common carriers that are subject to the jurisdiction of other regulatory agencies. In addition, the Safe Harbor principles may only be used for data transfers from the EU to the United States, so their applicability is limited. Moreover, in certain jurisdictions, and in most EU Member States, consent is strongly disfavored particularly when it involves the transfer of employee data because there is a view that consent cannot be given "freely" within the context of the employment relationship or in exchange for goods or services.[53] Also, if consent is required and a customer does not consent, then the organization may not be able to centralize its procurement functions to centrally ship the goods to all of its customers.

Despite the fact that each privacy law provides some means for transferring information, the divergent laws of the sixty or more countries make it virtually impossible for businesses to select a single safeguard to protect the data as they transfer data from one country to another. That is certainly the case in the EU,[54] where businesses must analyze and satisfy twenty-seven different standards for transferring information outside the EU, thus defeating the harmonizing intent of the EU Directive.[55] The European Commission acknowledged this difficulty in its first report on the implementation of the EU Directive, and stated: "more work is needed on the simplification of the condi-

53. Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 Oct. 1995, Art. 29 Working Party Doc. WP 114 (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

54. The EU Directive sets a floor for the Member States' legislation, and in some instances it may also set a ceiling. It does not, however, prohibit divergences among Member State laws. *See* Parliament and Council Directive No. 95/46 of 24 Oct. 1995, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

55. The only uniform method of complying across the EU is with standard clauses/model contracts. If a global organization, however, is elected to utilize model contracts to transfer data among affiliates, it is perfectly possible that it would have to enter into hundreds of contracts which would be administratively burdensome and complex.

tions for international transfers."[56] Thus, there is no standard means to comply with the cross-border transfer obligations even among the twenty-seven EU Member States, let alone among the sixty-plus countries with data protection laws that restrict cross-border transfers.

A. *Consent*

As mentioned above, organizations can legitimize the transfer of personal information from one country to another by obtaining the consent of the individual to transfer his or her personal information. In most EU Member States, for example, consent to transfer personal information to a country that has not been deemed adequate by the EU would need to be affirmative (opt-in) consent. Similarly, affirmative consent is usually required in countries such as Argentina, Korea, Mauritius, and the U.A.E. (DIFC). In other countries such as Australia and Canada, opt-out consent may be sufficient. Regardless of the form of consent required, almost all jurisdictions require that such consent be informed and as such, notice would need to be provided.

At first glance, consent appears likely to be an organization's simplest option for legitimizing its data processing practices as it could be drafted to cover all uses of the data. Authorizations also can be made relatively consistent across all countries, thereby enabling organizations to use a uniform, worldwide approach to data transfers.

This method, however, poses significant issues for an organization, particularly in the employment context. Whether "consent" may be freely given in the context of an employment relationship has been the subject of much debate among the EU Member States. Several EU Member States maintain the view that an existing employee cannot freely give consent. Moreover, the Working Party 29, the assembly of all twenty-seven EU DPAs, takes the view that:

> where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal information, it is misleading if the employer seeks to legitimize this processing through consent. Reliance on consent should therefore be confined to cases where the worker has a genuine

56. *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 19, COM (2003) 265 final (Feb. 24, 2004), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/com/2003/com2003_0265en01.pdf.

> free choice and is subsequently able to withdraw the consent without detriment.[57]

Similarly, the U.K. Information Commissioner recently issued revised guidance on international data transfers confirming that valid consent means that the data subject must have a real opportunity to withhold their consent without suffering any penalty.[58] Accordingly, in the EU Member States that take this position, an employer who relies on consent to legitimize data processing in the employee context may face significant risks and should consider other (additional) possibilities for transferring information.

Also, consent may provide at best only a short-lived solution for businesses because employees or customers may withdraw their consent at any time.

The advantages and disadvantages of a consent-based approach to cross-border data transfers can be summarized as follows:

Pros:

- *Choice:* Use of consent, particularly opt-in consent, is the most direct and, in some instances, the least risky means of legitimizing cross-border data transfers of personal information as the entities sending and receiving the data assume only the obligations delineated in the notice that forms the basis of the consent.
- *Consistency:* Consent can be relatively consistent across all countries.
- *Liability:* The receiving entity does not have to take on any liability for its information processing practices.
- *Audit:* Consent does not expose the entities receiving information to audit by the data protection authorities of the exporting country.
- *Compliance Burdens:* Consent is required in many instances to satisfy local compliance obligations. In Argentina, the EU Member States, Korea, Mauritius, Tunisia and the U.A.E., for example, any processing of "sensitive" data (i.e., specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex

57. Opinion 8/2001 on the Processing of Personal Information in the Employment Context of 13 Sept., 2001, at 23, Article 29 Working Party Doc. WP 48 (2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf.

58. Info. Comm'r's Office, Data Protection Guidelines: International Transfers of Information General Advice on how to Comply with the Eighth Data Protection Principle, at 9, a*vailable at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/general_advice_on_how_to_comply_with_8th_data_protection_principle.pdf.

life of the individual) usually requires consent. Also, in certain countries there are additional categories of sensitive information such as performance appraisals, criminal background checks and credit checks. Thus, adding a consent to transfer the data across borders can be relatively easy.

Cons:

- *Time and Expense:* Obtaining opt-in consent from all individuals (customers, employees, independent contractors and employees of vendors) is time consuming and costly. Obtaining consent to reflect changes in business needs may prove difficult.
- *Validity of Consent:* Several EU DPAs and in particular the Working Party have expressed doubt that truly voluntary consent can ever be given by employees and serve as a basis for international transfers.
- *Individual Choice*. Some individuals may refuse to provide consent and there can be no penalty associated with such a decision. Individuals are also permitted to withdraw their consent at any time. While this ability to repudiate consent strengthens the argument that individuals have genuine free choice, it might weaken the effectiveness of consent.
- *Form Requirements:* Some countries including Argentina, Germany, Korea, Mauritius, Tunisia and the U.A.E. require consent to be given in writing.
- *Adequacy Statement:* If an organization in the EU wants to transfer personal information to a country that has data protection that has not been deemed "adequate" by the EU, it is required to include a sentence in the notice to individuals that their information will be transferred to a country that may not ensure "adequate" privacy, which may discourage some individuals from providing consent.

B. *Contracts*

Use of contracts between the entity transmitting information and the recipient is another legitimate means by which to transfer personal information from one jurisdiction to another. In the EU, the European Commission has approved different sets of model contracts ("Standard Clauses").[59] When Standard Clauses were introduced it was hoped that

59. The Commission Decision No. 497/2001 of 15 June 2001, 2001 O.J. (L 181) 19, on standard contractual clauses for the transfer of personal information to third countries, under Directive 95/46/EC (2001/497/EC), incorporates the standard terms suggested by the European Commission for transfers to so-called controllers; Commission Decision No. 915/2004 of 27 December 2004, 2004 O.J. (L 385) 74, amended Decision 2001/497/EC as regards the introduc-

because they provided one form of contract useable in all EU Member States without further scrutiny by DPAs, they would allow for workable and substantially more streamlined international data transfers. Unfortunately, however, it appears that the drawbacks of Standard Clauses may outweigh their advantages.[60] Contracts that derogate from Standard Clauses require approval from most EU DPAs, which is a costly and lengthy process.

In Japan, there is no pre-approved model contract, but the Guidelines published by the Financial Services Administration contain detailed guidance relating to the provisions that should be contained in a contract with a service provider (either in Japan or in any other country).[61] Similarly, in Korea, there are no pre-approved clauses but entities and their agents are required to take necessary security measures, including technical and administrative measures to protect personal information and procedures to handle complaints and disputes.[62] In Argentina and the U.A.E., the laws explicitly, in the case of the former, and implicitly in the case of the latter, provide for the use of contracts as a way to legally transfer data outside the country but clauses have yet to be developed by the DPA.[63]

The main disadvantages of contracts are that they are administratively burdensome and only work in environments where the informa-

---

tion of an alternative set of standard contractual clauses for the transfer of personal information to third countries; and on 27 December 2001, the European Commission adopted Commission Decision (EC) No. 16/2002 of 27 December 2001, 2002 O.J. (L 6) 52, on standard contractual clauses for the transfer of personal information to processors established in third countries, under Directive 95/46/EC.

60. Besides entailing burdensome compliance requirements, the Standard Clauses require that individuals to whom the information relates are to be made third-party beneficiaries of the agreement, providing individuals with a direct cause of action and impose liabilities on both the exporter and the importer. *See* Commission Decision No. 915/2004 of 27 December 2004, 2004 O.J. (L 385) 74, 79. Further, an entity importing EU data may generally only provide the information to third parties if those third parties are subject to an adequacy finding, execute model contract clauses or consent is obtained by each and every individual. *Id.* at 78-79.

61. [Japanese Financial Services Administration General Guidelines on the Protection of Personal Information in the Financial Services Area], *available at* http://www.fsa.go.jp/common/law/kj-hogo/01.pdf; [Japanese Financial Services Administration Guidelines on the Security Measures for the Protection of Personal Information in the Financial Services Sector], *available at* http://www.fsa.go.jp/common/law/kj-hogo/04.pdf.

62. *See* PICNU, *supra* note 51.

63. *See* Law No. 25326, Oct. 30, 2000, [X] B.O. 30 (approved by Decree No. 1558/2001), *available at* http://www.jus.gov.ar/dnpdpnew/index.html; Data Protection Law 2007, DIFC Law No. 1 of 2007, *available at* http://www.dp.difc.ae/legislation/files/DP%20Law%201%20Jan%202007%20v14.pdf.

tion flow is stable and fairly limited. However, for most businesses, information flows do not follow neat or well-established paths, but travel along multiple paths through a multitude of channels, through e-mail exchange, access to databases, and intranets. Global organizations have complex organizational structures that can change frequently. Unless regularly revised—at considerable expense—contracts will not be able to reflect the changes in usage of information in organizations, as required under the contract regime.

The advantages and disadvantages of a contractual approach to cross-border data transfers can be summarized as follows:

Pros:

- *Legal Certainty.* In the EU, contracts have been used for almost 20 years. Regulators are familiar with them, and therefore contracts, and the Standard Clauses, can provide a great deal of legal certainty.
- *Individual Consent Not Required.* The organization can put contracts in place without seeking consent from each relevant individual.
- *Tailored Solution.* Contracts can reflect the data that is being moved and the activities that are being carried out in relation to that data.
- *Involvement of the DPAs.* Contracts do not require approval from DPAs in most countries other than the EU Member States. In the EU, in theory, Standard Clauses do not require prior authorization by individual DPAs either. (In practice, however, almost half of the EU DPAs do require businesses to file using the Standard Clauses "as an administrative formality" and obtain authorization for data transfers.)

Cons:

- *Administrative Difficulties:* Contracts can be difficult to administer as they are static documents and must be updated as organizational, technical and other changes are implemented and then reauthorized either by new signatures or new unilateral undertakings. If an organization relies on the use of ad hoc contracts, it will need to continue to track data received from the Member States by country of origin to ensure that the data is handled in compliance with the appropriate Member State data protection requirements.
- *Involvement of DPAs:* In the EU, any contract derogating from the Standard Clauses requires approval, which generally takes a minimum of one to two months and may take longer if the DPA has questions about the transfer or the requisite forms were not completed properly in the first instance. Subsequent additional approvals also may be required if changes are made in the processing or type of personal information collected.
- While prior approvals are not required for Standard Clauses,

almost half of the EU Member States (i.e., Denmark and the Netherlands) require that such contracts be registered prior to the contract being relied on as a cross-border mechanism. Although the DPAs are technically precluded from requesting changes to the terms of the Standard Clauses, a DPA can request amendments and additions to the appendices.

- *Non-EU Jurisdictions.* Standard Clauses will not necessarily meet all of the cross-border requirements in non-EU jurisdictions, such as Japan, Australia and Argentina; at the same time, an organization may have to provide protections greater than those required in non-EU jurisdictions.

C. *Adequacy Decisions*

Another option for transferring data is to rely on an adequacy decision. As mentioned earlier, the EU has issued a limited number of adequacy decisions, including one in 1998 for the U.S. Safe Harbor Privacy Principles ("Safe Harbor"), which provides an alternative basis for data transfers to the United States.

For a U.S. organization to be eligible for the Safe Harbor, it must be subject to the jurisdiction of a "government body which is empowered to investigate complaints and to obtain relief against unfair and deceptive practices. . .in case of noncompliance with the [Safe Harbor] Principles."[64] At present, only the FTC (under section 5 of the Federal Trade Commission Act ("FTC Act")) and the DOT (under 49 U.S.C. § 41712, which covers air carriers)[65] are recognized by the European Commission as satisfying this requirement. Therefore, only organizations subject to the jurisdiction of either of those two agencies are eligible to join the Safe Harbor.[66] Thus, financial institutions, telecommunications, and several other regulated entities are not able to utilize the Safe Harbor.

The Safe Harbor provides *one* privacy regime for all EU personal information that is transferred to the United States. It eliminates the

64. Commission Decision No. 518/2000 of 26 July 2000, art. 1(2)(b), 2000 O.J. (L 215) 1 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_215/l_21520000825en00010003.pdf.

65. The EU wanted to ensure that a government body (state or federal) would provide Safe Harbor enforcement in the event that self-regulatory mechanisms did not operate appropriately. To date, only the FTC and DOT have agreed to enforce the Safe Harbor.

66. Financial services institutions that are subject to the jurisdiction of the banking regulatory agencies and telecommunications common carriers (which are subject to the jurisdiction of the Federal Communications Commission) are not eligible for the Safe Harbor at this time.

need for prior approvals or makes them automatic. As a result, the Safe Harbor can provide a streamlined approach for data transfers from the EU and can make those transfers less expensive and less onerous. In addition, the Safe Harbor requirements are interpreted in accordance with U.S. law, which imputes a reasonableness standard to the Safe Harbor's terms. The Safe Harbor, however, only applies to transfers of data from the EU to the U.S. and, thus, it is not a global solution. The same is true for the other adequacy decisions issued by the EU. The rest of the world is left out.

Pros:

- *Consistency*. Reliance on an adequacy decision would harmonize transfers of personal information between adequate countries, subjecting such information to a common privacy regime.
- *Compliance Burden*. Transfers to countries or entities that are subject to an adequacy decision eliminate the need for prior approvals from EU DPAs or make such approval automatic.
- *Familiarity*. With respect to the Safe Harbor, the Safe Harbor more clearly reflects the U.S. approach to privacy and to some extent the moderate requirements of the EU Directive.
- *Public Relations*. Referring to the Safe Harbor or transferring to a country with adequate data protection can have a positive PR effect.

Cons:

- *Limited Applicability*. Adequacy decisions are only applicable to individual countries or, in the case of the Safe Harbor, to organizations that certify to the Safe Harbor. Therefore, these authorizations may only be used for transfers between the EU and the country subject to the particular authorization. Also, in the case of the Safe Harbor, it is not available to financial institutions or providers or telecommunications services.
- *Involvement of the DPAs*. For the Safe Harbor to cover an organization's employment data, the organization must agree to cooperate with the EU DPAs as the complaint resolution mechanism.
- *Compliance Burden*. For the Safe Harbor, organizations have to recertify to the Safe Harbor every year.

IV. Problems with the Current Compliance Alternatives

Unfortunately, the existing patchwork of cross-border rules has done little to provide real protection for individuals' personal information. At the same time, these cross-border rules, by virtue of the fact that they are making such transfers more difficult and costly, are adversely affecting the quality and choice of products and services that can be offered to consumers on a global basis.

A. *Illusory Protection for Individuals*

Individuals and, in particular, consumers, are ill served in the networked economy because their personal information is not protected in a uniform and consistent manner. If a problem arises, such as, for example, they are a victim of identity theft or their personal information is shared with third parties against their wishes, the consumer must determine who is at fault, what laws apply, what his or her rights are with respect to the standard of protection in that jurisdiction, and who needs to be contacted to have the problem resolved. The answer to these questions may be complex given the multi-jurisdictional nature of data flows and the potential applicability of one or more sets of national rules. Even after these questions are answered, consumers may not be able to resolve the problem depending on how well law is enforced in a given country (or countries). Differences in language may further complicate the matter. At the same time, consumers depend on the international flow of information because it gives them access to a wider array of information as well as goods and services at lower prices, and enables them to receive customer service twenty-four hours per day.

The following are some examples that illustrate the illusive nature of the privacy protections afforded to consumers by the current international regime.

No effective recourse mechanism

A U.S. consumer purchases a product over the Internet from a German company that is an affiliate of a U.S. company. The German company fails to properly secure the personal information of the individual and the U.S. consumer becomes the subject of identity theft. What recourse does the U.S. consumer have against the German company?

The FTC has no jurisdiction over a German company doing business in Germany.[67] The U.S. affiliate has no legal authority to compel the German affiliate to take any particular activities. The U.S. consumer (if he or she can speak German) could call and file a complaint with the German DPA, but it is unlikely that the German DPA will take any action based on an issued raised by a U.S. consumer. Thus the U.S. consumer effectively has no recourse.

---

67. The FTC's enforcement authority is limited to those organizations covered by Section 5 of the FTC Act. *See* 15 U.S.C. §§ 41-58 (2000).

Privacy breach occurs but no privacy law is violated

*A U.S. consumer is on vacation in Europe. The consumer asks the hotel where he is staying to make reservations for him at two other associated hotels in Asia and Latin America. At the consumer's request (*e.g.*, with his consent), the European hotel transfers personal information about the consumer to the other hotels such as his name, address, and meal preferences, which reveal his religion and credit card information. The hotel in Asia, located in a country that has a privacy law that contains very limited security obligations, fails to properly protect the information and the consumer becomes a victim of identity theft. In addition, the hotel in Latin America, located in a country that has no privacy laws in place, may sell its customer information to data brokers and the information is then used for other purposes. Who is at fault for these privacy violations? What rights and recourse does the consumer have?*

In this scenario, the consumer has no rights or guarantees that his personal information will be protected because he consented to the transfer. The European hotel did not violate European privacy laws because it transferred the information with the consent of the individual. It is not legally responsible for any misuse of that information by other hotels in its international chain. The Asian hotel is also not liable for any damages because it has minimal security safeguards in place that technically satisfy the local requirements (although they may fall far short of security requirements in jurisdictions with more rigorous standards). The hotel in Latin America is not liable because it is located in a country that has no privacy laws and therefore is also not limited to how it may use the data. Thus, the consumer has no recourse.

Unable to determine who is at fault

A U.S. consumer uses a credit card to purchase a computer product from a U.S. company. The customer's personal information will need to be shared with two different affiliates within the company: one for warranty purposes and the other for customer service purposes. These affiliates are located outside the U.S. The company's U.S. privacy policy discloses that customer information will be shared with affiliates of the organization for those purposes and the U.S. company will safeguard the personal information that it processes in the U.S. It refers the customer to the privacy policies of its affiliates for information about how those entities protect customer information. A hacker then breaks into the company's global computer system and steals customer information. Which entity is at fault? What rights and recourse does the consumer have?

It may be extremely difficult, even with superb computer forensics, to determine at precisely which point in the global network a hacker found entry. If it cannot be determined where in the system the

hacking occurred, or if the hacker was from a completely different country and the information was collected in transmission between two affiliated entities, then it will be impossible to assign fault or responsibility for the security breach. Given that none of the affiliates will be responsible, each can avoid liability and the consumer is left completely unprotected and with no viable recourse mechanism.

Delayed or cumbersome access to customer service

A U.S. consumer purchases a computer from a U.S. company and has trouble setting it up. Over a one-week period, the consumer has to call the company's customer service support hotline at three different times of the day. Calls to the hotline between 9:00 a.m. and 9:00 p.m. EST are handled by the U.S. company, between 9:00 p.m. and 3:00 a.m. EST by its Japanese affiliate, and between 3:00 a.m. and 9:00 a.m. EST by its Irish affiliate.[68]

In order to provide this service and comply with the various national privacy laws, the company must either require the customer to repeat the same information about his problem (and provide service warranty information) every time he calls customer service or, to avoid such repetition, put into place four different contracts that will enable information to be shared among the affiliates. If the company opts for the latter approach, then the Irish affiliate must enter into a contract with the Japanese affiliate to transfer the data to it; the Irish affiliate must also enter into a contract with the U.S. affiliate or the U.S. affiliate must certify to the Safe Harbor. The Japanese entity must also enter into contracts with the Irish and the U.S. affiliates.

*Even with such contracts in place, the customer service representatives will still need to provide the customer with two verbal privacy notices before they can begin to address his problem. For example, the customer calls at 6:00 a.m. EST time and the Irish affiliate receives the call. In order to access the customer's purchase information to find out, for example, whether the customer purchased a service contract, the Irish customer service representative must provide a verbal privacy notice to the individual, describing the types of information collected, the purposes of the collection, with whom the information will be shared, the security measures taken to protect the information, the methods of keeping the data accurate, and the process by which the personal information can be corrected. The Irish customer service representative then collects additional information from the U.S. customer (*i.e.*, the nature of the problem, information about the printer*

68. As it is prohibitively expensive and extremely difficult to find qualified individuals to staff a customer service department in the United States twenty-four hours per day, the U.S. company has opted to set up customer service centers in other parts of the world so that they can retain qualified individuals and provide twenty-four-hour customer service.

that is being attached to the computer and the individual's phone number for a call back). The next day, the customer has an additional problem at 11:00 p.m. EST and the call is answered by the Japanese affiliate. The Japanese customer service representative will need all of the information that has been collected to-date and may collect additional personal information. But, before the Japanese customer service representative can access the account information, he or she must provide a verbal privacy notice similar to that provided by the Irish representative. The customer then calls a third time at 11:00 a.m. EST and speaks with a U.S. customer services representative. Depending on the U.S. company's privacy policy, the customer could conceivably hear a third privacy notice.

The customer will be extremely frustrated that he must hear the privacy notice each time and will likely be equally frustrated that he must provide his relevant data each time a customer service phone call is placed. For the company, the costs associated with establishing this type of customer service system is enormous. For example, an organization with offices in 15 EU Member States, Japan, the U.S., and Canada that wants to have a centralized customer data base to provide global customer services to its clients, would be required to enter into 108 separate contracts among the corporate affiliates and to have 18 different privacy notices. The cost of compliance is so administratively burdensome and so expensive that it may be easier simply to not provide twenty-four-hour customer service.

Diminished services and choice

A U.S. consumer wants to travel to Argentina and calls a U.S. travel agency. The U.S. consumer is not interested in the travel agency's group travel packages and instead wants a customized itinerary for independent travel through Argentina. Because the U.S. travel agency does not have all of the information requested by the consumer, it wishes to provide the consumer with the name and address of a travel agent from its affiliated travel agency in Argentina. What has to happen for the business contact information to be provided to the U.S. consumer?

In order for the U.S. travel agent to provide the business contact information of the Argentinean travel agent to the customer, the affiliated Argentinean travel agency would be required to give a notice to the individual Argentinean travel agent informing him or her that personal information is going to be collected and sent to the U.S. so that a referral can be made, that U.S. travel agents will have access to the information and that the information may be provided to customers in the U.S. In addition, it is likely that the individual travel agent in Argentina will have to consent to the provisions in the notice. Thus, the

U.S. and Argentinean travel agencies would need to keep track of and ensure that each relevant travel agent in Argentina receives a notice and consents to the collection, use and disclosure of his or her business contact information. In addition, if any one of the Argentinean travel agents withdrew his or her consent, the U.S. travel agent would have to be informed and the information relating to that travel agent would have to be removed from the database maintained by the U.S. travel agency. As a result, the U.S. and Argentinean travel agencies might decide that it was too difficult to manage the notices and consents. Under those circumstances, the U.S. travel agent could tell the consumer that no other information was available or provide the main telephone number and address of the Argentinean agency without providing the name of an individual travel agent. The travel agency may then lose the potential business if the consumer looks for another travel agency that can help locally. Alternatively, if the consumer decides to call the Argentinean agency directly, it might take several calls to identify the appropriate agent who can assist, an experience that will likely frustrate and annoy the consumer and undermine the overall business relationship with that consumer.

B. *Regulatory Burden for Organizations*

Businesses are also ill served by this patchwork regime. Businesses are eager to offer consumers a wide array of goods and services at competitive prices and provide customer service 24 hours per day. To do that, they need to manage their global operations in the most cost effective way possible which generally means that they will centralize certain functions throughout the entire organization (e.g., one affiliate may be responsible for processing all of the organization's human resources data, another would maintain the marketing/sales database, and a third affiliate may be responsible for managing the vendor database). As a result, the organization will need to transfer both non-personal information, such as inventory data, as well as personal information, such as customer, vendor and employee data, to their operations around the world. While such transfers are necessary to manage the business in an efficient manner, they also permit the organization to offer, for example, customer service to consumers twenty-four hours per day, by relying on customer service representatives from different time zones to "come online" at different times to assist customers who may be located halfway around the world. To be effective and convenient for the customer, these customer service representatives must have access to the organization's databases containing customer information such as the customer's credit, purchase and repair records.

They also need access to the organization's employee data so they can, for example, direct any required follow-up service to the correct office or dispatch the appropriate repair technician.

While organizations are striving to meet consumer demands for convenience and lower prices for goods and services, they are facing an increasingly complex burden to comply with both local and cross-border privacy rules in more than sixty different jurisdictions around the world.[69] In particular, as discussed below, cross-border rules are having the following impact on business operations.

Greater administrative burden

Managing the contracts among affiliated entities or obtaining workers' consents imposes an enormous administrative burden on companies. Any given organization may need to manage hundreds or thousands of contracts depending on how many affiliates the organization has at the time. In addition, anytime there is an organizational change among the parties to the contract (e.g., a different affiliate is assigned responsibility for processing human resources data for a given affiliate or possibly on an enterprise-wide basis), new contracts will need to be negotiated. Or, if the organization relies on consents, then it must permit the individual to withdraw consent at anytime and keep track of those preferences.

Increased jurisdictional conflicts

Reliance on contracts may increase the chances for jurisdictional conflicts of law, particularly with the advent of the Internet. To run a global business and to transfer information to affiliated entities to achieve coherent customer services, organizations that rely on contracts must enter into contracts with each affiliated entity. Many countries require that the law of the country from which the data is being

69. In addition to the cross-border compliance obligations previously discussed, there are extensive local compliance obligations. For example, all of these privacy laws impose notice obligations that require organizations to provide information to individuals about what personal information is being collected, the purposes for which it will be used, and the identity and location of the organization collecting and using the information. Each country generally has a different set of required elements that must be contained in the notices. In addition, some countries require organizations to update such notices on an annual basis while others require new notices whenever there is a slight change in the data being collected or its intended purpose or use (e.g., the organization changes from one service provider to another that may be located in a different country). Consequently, for large global organizations, thousands of new notices must be generated.

exported must be the law that controls the contract and the jurisdiction in which disputes must be heard. Thus, data that is transferred from Japan to France must be governed by Japanese law and data that is transferred from France to Japan must be governed by French law. In theory, to ensure compliance with all of the legal obligations, the data of each organization should be segregated based on the country of origin. In addition, with the advent of the Internet, if data is entered into a global database in Bangladesh and is instantly available in the fifty offices in which the organization has offices, it is not clear which contract or which countries' laws would be applicable. Consequently, if a breach involves multiple jurisdictions or it is not clear where the breach occurred in the network, it will be complicated to untangle the jurisdictional and choice of forum issues and would likely delay resolution of the issue.

Decreased business flexibility

The current system reduces business flexibility and inhibits businesses from managing their operations in an effective and efficient manner, which, in turn, impacts the range and price of products and services offered to consumers. In particular, the existing arrangement discourages or impedes enterprise-wide initiatives in such areas as training, succession planning, expense management, security, payroll, and provision of stock options. Given the complexity and administrative burden of obtaining workers' consents to transfer their personal information, some organizations opt to implement such programs locally which makes it difficult to ensure the same level of standards are followed at the local level as well as achieve the same economies of scale that could be achieved if the program were operated on an enterprise-wide basis. With respect to expense management, for example, if organizations were able to track and manage expenses on an enterprise-wide basis, they might be better positioned to negotiate larger discounts with suppliers and control their costs more effectively.

In addition to these administrative challenges, organizations must also grapple with conflicting cross-border transfer requirements in areas such as security that can make it difficult or impossible for them to develop systems best suited to their needs. For example, differences in security requirements could deter an organization from developing a harmonized and centralized security system on an enterprise-wide basis which, depending on the structure of its business, might provide better security protection than security systems at the affiliate level, each with different standards of security protection.

Workers are also disadvantaged by these restrictions on cross-border

transfers, particularly with respect to succession planning and stock options. If personal information is not transferred, then workers may lose out on valuable company benefits or promotional opportunities.

V. The Emerging Global Solution: Corporate Privacy Rules

Given the problems inherent in the existing approaches to cross-border data transfers, the concept of Corporate Privacy Rules is emerging as a new and better approach to managing global data transfers. Under Corporate Privacy Rules, an organization would apply just one set of rules to govern data transfers among all jurisdictions. Both the parent and its affiliates are bound to protect the information according to those rules. The organization would then be able to move data as required among participating jurisdictions pursuant to these rules. The organization would still be responsible, however, for complying with the local data protection requirements (e.g., database registration, notice and access rights), if any, in each of the participating jurisdictions for the collection, use and disclosure of personal information within the individual jurisdictions.

If a breach occurs, the affected individual will be able to file a complaint locally in his or her native language—regardless of where the breach occurred or which affiliate was responsible for the breach—and have the complaint addressed in an appropriate manner by the company with whom he or she has a relationship. In short, a breach by one affiliate would be treated the same as a breach by any other, so individuals would be provided with consistent and enforceable rights, even in jurisdictions with no privacy laws in place.

To understand how such rules would work in practice, consider the following scenario:

An individual located in Europe provides personal information directly to an affiliate located in Asia or indirectly through its local European affiliate. The Asian affiliate mishandles the information (violating the organization's Corporate Privacy Rules).

Rather than force the individual to resolve the problem directly with the Asian affiliate and have to contend with different time zones as well as linguistic and cultural differences, the individual would be able to contact his or her local affiliate to file a complaint. The local (European) affiliate would be responsible for resolving the problem within the organization and would serve as the local interface with the individual. How the organization chooses to resolve the problem internally (e.g., determine which entity is financially or legally responsible) would be for the organization to decide.

If the individual is unable to resolve the problem with the local

entity, the individual would then be directed to an independent dispute resolution body authorized by the organization to hear and resolve complaints. If the issue was not resolved to his or her satisfaction, the individual would still be able to pursue legal claims against the organization or file a complaint with the authorities in the jurisdiction in which its Corporate Privacy Rules were approved or certified. As discussed *infra*, there should be a logical connection between the designated jurisdiction and the organization's operations (e.g., the jurisdiction selected might be the jurisdiction in which it has its center of activity or in which it is headquartered).

A. *Benefits Of This Approach?*

Individuals

Corporate Privacy Rules offer significant benefits to individuals. They offer an effective method of protecting personal information no matter where the data is located throughout the world. Corporate Privacy Rules can ensure consumers' personal information is accorded a uniform level of protection, eliminate the need to determine the legal regime applicable to data processing activities in multiple countries, particularly with respect to on-line transactions, provide a local recourse mechanism, and simplify and reduce the cost of data privacy compliance for cross-border transfers, thereby encouraging greater compliance.

In the context of the consumer examples cited in Section IV *supra*, the benefits of Corporate Privacy Rules to individuals become apparent:

1. *Corporate Privacy Rules Can Provide the Consumer with More Effective Recourse Mechanisms*

In the example involving a U.S. consumer and a German company, the U.S. consumer would be able to call the offices of the U.S. entity and file a complaint locally (and in English) if the parent has Corporate Privacy Rules in place. Consequently, the U.S. consumer would have recourse that it would not otherwise have if it had to deal directly with the German company. Moreover, the FTC would be able to exercise its jurisdiction through the U.S. entity if the German company failed to address the complaint.

2. *Corporate Privacy Rules Provide Consumers with Consistent and Enforceable Rights Even in Jurisdictions with No Privacy Laws in Place*

In the hotel example, the hotels located in countries with less

stringent or no privacy laws would be required to abide by the same privacy rules of all the other hotels in the chain. As a result, the U.S. consumer's privacy rights will not change from one jurisdiction to another and the consumer has the assurance that his or her personal information will be protected in a consistent manner by all of the hotels in the organizational group. In the event that there is a breach or unauthorized use of the consumer's personal information, the consumer will be able to file a complaint with any of the hotels in the chain and have the complaint addressed in an appropriate manner.

3. *Corporate Privacy Rules Eliminate the Need to Determine Which Entity is at Fault*

In the example involving the purchase of a computer product, the organization as a whole is responsible for protecting the data regardless of which affiliate processes the data. A breach by one affiliate is treated the same as a breach by any other affiliate. The consumer's rights and recourse are protected no matter where the breach occurs.

4. *Corporate Privacy Rules Facilitate Twenty-Four-Hour Customer Service*

Corporate Privacy Rules would enable organizations to provide seamless twenty-four-hour customer service. Consumers would not need to receive multiple privacy notices. Their customer history files would be accessible to any customer service representative in any location, thereby eliminating the need to have the customer repeat his or her problem with the product. By eliminating the privacy compliance costs associated with global data transfers, more companies might implement twenty-four-hour customer service hotlines.

Businesses

From a business perspective, Corporate Privacy Rules are attractive because they would enable organizations to implement uniform privacy policies and practices on a regional or global basis without the administrative, legal, and organizational complexities of contracts. Moreover, these rules can be tailored to the needs of a particular business or industry sector, taking account of particular challenges and sensitivities, the corporate culture, processes, and the organizational structure. In addition, Corporate Privacy Rules could further encourage best practices and, in particular, the training and education of the workforce regarding privacy rules and expectations. Companies would be able to institute a single organization-wide program rather than

replicate the program in multiple local markets. Corporate Privacy Rules could also translate abstract obligations into a "real life" context without any legalese, and thus help the workforce understand and implement their respective obligations.

Implementing Corporate Privacy Rules is simply an extension of an approach that has worked successfully in other areas. It is not a new concept. For years, businesses have developed and enforced enterprise-wide policies in a variety of areas (e.g., in the field of financial reporting, determination of codes of conduct, and conflicts of interest). For these reasons, we believe that Corporate Privacy Rules could offer a new approach for consumers and organizations that will promote a more comprehensive culture of privacy.

B. *Moving Toward the Development of Corporate Privacy Rules*

Currently, there are two separate initiatives underway in different regions of the world that are developing new ways to facilitate cross-border data transfers:

EU Approach

In the EU, Corporate Privacy Rules take the form of binding corporate rules ("BCRs"). The main current features of BCRs are outlined by the Working Party 29 in papers issued in 2003 and 2005.[70] As envisioned by the Working Party 29, organizations would be required to comply with the strictest EU national regimes in order to use BCRs. The organization would be required to select and contact a "lead authority" and then present its draft BCRs in English as well as the language of the lead authority, together with sufficiently detailed information on the organization's structure, data flows, etc.

The lead authority would generally be the DPA in the jurisdiction where the organization is headquartered in the EU, or where the person with overall responsibility for the definition and implementation of the data processing is located or the jurisdiction from which most data are transferred or from which most processes are controlled.

---

70. *See* Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules", Article 29 Working Party Doc. WP 107 (Apr. 14, 2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm. *See also* Transfers of Personal Information to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Article 19 Working Party Doc. WP 74, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf.

This authority would work with the other regulators in other relevant Member States. One Member State would not, however, have the ability to approve the rules without consultation with other Member States. Because the proposed mechanism for regulatory approval is purely voluntary, national authorities may refuse to co-operate either generally or with respect to the approval of a particular set of rules.

In January 2006, the U.K. Information Commissioner approved the first set of BCRs for the transfer of personal information by the General Electric Company to countries outside the EEA without an adequate data protection regime in place.[71] Nonetheless, a large number of EU Member States remain either lukewarm or hostile to BCRs because of concerns relating to the enforceability of BCRs.

Given the discussion above, it is apparent that important obstacles still remain to the widespread adoption of BCRs within Europe. In particular, the lack of a streamlined mechanism for obtaining regulatory approval of BCRs and the fact that these authorities can request changes to the BCRs reduces the likelihood that a single set of rules can be implemented. If an organization must comply with the strictest obligations in each Member State in which it operates, any "balancing" mechanisms that currently exist within national legislation may be lost. For example, different national regimes often have different focuses, e.g., strict surveillance may be compensated for by less strict internal audit requirements or broad statutory exemptions under which data may be processed may be complemented by a very narrow interpretation of what constitutes valid consent. Forcing organizations to adhere to a combination of the strictest regimes may deter them from adopting BCRs.

Further, many Member States have adopted differing views on the binding nature of BCRs and in some Member States, such as Spain, there is no provision in the law for recognizing binding corporate rules. To achieve widespread practical usage, EU data protection authorities will need to harmonize their individual approaches to BCRs.

Ideally, each Member State should recognize and give full effect to a set of BCRs approved by another Member State DPA (which could be the authority of the country in which the data controller has its "centre of activities"). To accomplish this, the Member State authorities would need to agree to recognize the regulatory authority of the country

71. *See* Info. Comm'r's Office, Binding Corporate Rules Authorisation (2005), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/binding_corporate_rules_authorisation%20_final.pdf.

where a transaction takes place, as well as the country from which a product, a person, or a service originates. This, in turn, embodies the principle that if a service can be provided lawfully in one jurisdiction, it can be provided freely in any other participating jurisdiction, without having to comply with the regulations of the other jurisdictions.

In this respect, it is important to bear in mind the common denominator of BCRs—to ensure that the data is adequately protected. The goal is not to afford protection equivalent to every Member State's privacy regime. The EU Directive does not require that BCRs provide more protection than that offered by other adequacy mechanisms established in the EU Directive; rather, it only requires that BCRs provide adequate protection.

APEC Approach

In November 2004, the Asia Pacific Economic Cooperation ("APEC") Member Economies[72] approved a regional privacy framework that would permit the use of Corporate Privacy Rules to transfer personal information easily throughout the region.[73] This APEC Framework is also intended to promote a consistent approach to information privacy protection across APEC Member Economies, while avoiding the creation of unnecessary barriers to information flow. Creation of the APEC Framework also contributes to broader APEC e-commerce objectives to increase cross-border trade and growth in e-commerce in the region. In addition, APEC Ministers endorsed a Future Work Agenda on International Implementation of the APEC Privacy Framework, which includes instructing APEC members to continue efforts to develop a regional approach to privacy that will support global business models, such as privacy codes.[74]

The APEC Framework, which consists of a set of privacy principles ("Privacy Principles") and implementation guidance, seeks to achieve

---

72. The APEC Member Economies are Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Viet Nam.

73. *See* Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), http://www.apecsec.org.sg/apec/apec_groups/som_special_task_groups/electronic_commerce.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

74. *See* Asia-Pacific Economic Cooperation, Electronic Commerce Steering Group, *Future Work Agenda: Privacy Subgroup*, 2004/SOMIII/ECSG/024 (Sept. 29-30, 2004), *available at* http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2004.html.

four main goals:

- To develop appropriate privacy protection for personal information;
- To prevent the creation of unnecessary barriers to information flow;
- To enable multinational businesses to implement a uniform approach to the collection, use and processing of data; and
- To facilitate both domestic and international efforts to promote and enforce information privacy protection.

The APEC Framework is intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. It highlights the reasonable expectations of consumers that businesses will recognize their privacy interests in a way that is consistent with the Privacy Principles outlined in the APEC Framework.

In general, the nine Privacy Principles are closely aligned with those found in the 1980 OECD Privacy Guidelines[75] and cover notice, choice, collection limitation, use of personal information, data integrity, security safeguards, access and correction, and accountability. The accountability principle, however, goes further than the OECD accountability principle by stating explicitly that when transferring information, whether domestically or internationally, organizations that control the collection, holding, processing or use of personal information should be accountable for ensuring that the recipient organization will protect the information consistently with the Privacy Principles when not required to obtain consent. The goal of the accountability principle is to enable organizations to develop and implement uniform approaches within their organizations for global access to and use of personal information.

Work on the implementation phase is underway. In particular, Member Economies have agreed to:

- Develop a multilateral mechanism for promptly, systematically and efficiently sharing information among APEC Member Economies;
- Develop cooperative arrangements among privacy investigation and enforcement agencies of Member Economies; and

75. *See* Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

- Endeavor to support the development and recognition of organizations' cross-border privacy codes across the APEC region.[76]

The next round of APEC privacy meetings were held in late January 2007 in Australia. During those meetings, Member Economies were expected to continue their efforts to support the development and recognition of Corporate Privacy Rules and continue to work on ways to implement the APEC principles in the Member Economies.

C. *Where Do We Go From Here?*

At present, it is unclear if and how the initiatives in the EU and APEC can come together to achieve a global solution to international data transfer issues. One thing is clear, however: regional solutions alone will not be sufficient to resolve this issue. For Corporate Privacy Rules to become a reality, governments will need to recognize their value and make them a priority. While the initiatives in the EU and in APEC are laudable, regional solutions do not address the need for free information flow while protecting privacy, let alone the reluctance of some EU DPAs to commit to a pan-European solution.

A solution will require creative thinking about how to implement transfers in their respective jurisdictions as well as a strong commitment to work closely with other governments to devise an approval process that will be acceptable to all. In many, if not all of the jurisdictions, the proactive involvement of data protection, privacy authorities, consumer protection agencies and other relevant agencies will be required.

The key to any solution is that, apart from being truly global, it must also provide a method of implementing one set of rules throughout the world. As demonstrated above, the cost—both from a business and a consumer perspective—of divergent cross-border solutions is too high. What is needed is a method of adopting and being bound by one set of rules that can be uniform across the globe and is deemed sufficient in every jurisdiction. In the following sections, we lay out a possible roadmap for implementing and enforcing Corporate Privacy Rules.

VI. Corporate Privacy Rules: Implementation Overview

Any business that intends to implement Corporate Privacy Rules

76. *See* Asia-Pacific Economic Cooperation, *APEC Privacy Framework International Implementation ("Part B") Final—Version VII*, 2005/SOM3/ECSG/020 (Sept. 8-9. 2005), *available at* http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.html.

would have to develop a set of rules to incorporate internationally accepted principles of fair information practices, such as the APEC Privacy Principles. The Corporate Privacy Rules would be evaluated and "certified" to ensure full compliance with these principles. For example, the Corporate Privacy Rules should be evaluated to ensure that they prescribe disciplinary sanctions for employees who violate the rules, allow for training on the Corporate Privacy Rules, and appointment of a Chief Privacy Officer and/or local privacy officers to further promote internal compliance. As will be further examined below, the certification could take the form of attestations/self-declaration or review by designated public or private entities to determine if the Corporate Privacy Rules comply with the internationally accepted set of principles.[77]

After completion of the certification procedure, the business would issue a public declaration of its adherence to the Corporate Privacy Rules or submit the rules to an appropriate DPA that would render the Corporate Privacy Rules enforceable, and a promise by the business to follow the policies established. The public declaration would be by the entire "corporate family"[78] or any affiliated entities that wished to share data. A complaint handling procedure would be developed to detail the manner in which complaints should be addressed.

The business would also need to undertake a comprehensive self-audit of its information processing practices in order to ensure that the practices are in accord with the stipulations in the Corporate Privacy Rules. Each business would then be obligated to regularly review its practices to ensure compliance with the requirements of the Corporate Privacy Rules.

Once these steps have been completed, the Corporate Privacy Rules would be regarded by all of the participating jurisdictions as satisfying the cross-border data transfer requirements of each jurisdiction without the need for further authorization or regulation. The business would then be able to move information as required to meet its needs among participating jurisdictions pursuant to its Corporate Privacy Rules. The business would still be responsible for complying with the local data protection requirements (e.g., database registration, notice

77. Whether the business in fact lives up to the promises made in its Corporate Privacy Rules would not be a matter to be determined at the certification stage. Rather, that would be determined by self-audit or through a third party audit procedure if a complaint is received and is not resolved through the internal complaint procedure.

78. The mechanism to ensure that Corporate Privacy Rules are binding upon all members of the corporate group will depend on the jurisdiction.

and access rights), if any, in each of the participating jurisdictions for the collection, use and disclosure of personal information within the individual jurisdictions.

A. *Certification Process for Corporate Privacy Rules*

There are several different models possible for certifying Corporate Privacy Rules. While each jurisdiction should have the ability to select the certification model best suited for its own jurisdiction, the model used across participating jurisdictions would need to be consistent and uniform to ensure credible and predictable enforcement.

1. **A business could self-certify that its Corporate Privacy Rules comply with a set of internationally accepted privacy principles.**

The self-certification would involve an internal assessment of the Corporate Privacy Rules to ensure that the rules are in accord with the APEC Framework or other internationally accepted principles of fair information practices. The business would be required to self-certify compliance with these principles.

2. **A business could submit its Corporate Privacy Rules to a designated private or public entity for approval.**[79]

If a designated private or public entity reviews the Corporate Privacy Rules to ensure that they comply with the Privacy Principles or other internationally accepted principles of fair information practices, its compliance review might involve verification that there is an online privacy policy posted that covers the Privacy Principles or other internationally accepted principles of fair information practices and the designation of a dispute resolution mechanism.

A hybrid approach may include the development of an approval or verification process by public sector entities, which would be carried out by authorized private sector entities. Such a process could include guidance in the form of checklists or other documents that set forth essential code aspects or factors to satisfy the verification process. While there is a desire to obtain consistent outcomes in the verification process, some flexibility must be maintained to allow for variances in business models, customer bases, sectors and legal frameworks.

---

79. If a nonprofit organization carried out these functions, the regulatory body would need to give priority to referrals of non-compliance with guidelines that govern private organizations. If these private organizations fail to carry out their responsibilities (e.g., they approve Codes without undertaking the proper due diligence), their conduct would be actionable, in the case of the United States, under the FTC's unfair and deceptive trade practices authority or enforcement authority of other regulatory bodies.

B. *Public Declaration*

There are also different ways in which businesses might make public declarations that would then be enforceable together with a promise to follow the policies in its public declaration. For example, consider the following options:

1. **A business would make a public declaration that it will protect personal information that it transfers from one jurisdiction to another in accordance with its approved Corporate Privacy Rules.**

The declaration could be included in the organization's privacy policy or some other public statement that is posted on its website (or in the case of workers, on its intranet). The organization would need to designate or indicate the jurisdiction in which it is certifying its set of Corporate Privacy Rules. There should be a logical connection between the designated economy and the business's operations (e.g., the jurisdiction selected might be the jurisdiction in which it has its center of activity or in which it is headquartered).

2. **A business would make a public declaration that it will protect personal information that it transfers from one jurisdiction to another in accordance with its Corporate Privacy Rules by registering its commitment with a designated private or public entity.**

The declarations/registrations would be submitted by the business to a private or public body and would then be available online for public inspection.

Once a business makes a public declaration, then its Corporate Privacy Rules would be regarded by all of the other participating jurisdictions as satisfying the "cross-border" data transfer requirements of each participating jurisdiction without the need for further authorization or regulation. The business could then move data as needed among participating jurisdictions pursuant to its Corporate Privacy Rules. The business would still be responsible, however, for complying with the local data protection requirements (e.g., database registration, notice and access rights), if any, in each of the participating jurisdictions for the collection, use and disclosure of personal information within the individual economies.

C. *Complaint Handling*

Those businesses that elect to participate in a Corporate Privacy Rules process would provide information about their complaint handling procedure in either their privacy policy or other documents that

are made available to the individual concerned. This information would detail the manner in which and to whom complaints should be addressed, the existence of any third party dispute resolution mechanisms, and the regulatory authority or agency that would receive complaints from individuals once all other dispute resolution mechanisms have been tried.

Complaints about any handling of personal information would be addressed, first, through the business's internal complaint handling process. If the complaint cannot be resolved internally, then the business is strongly encouraged to have an independent dispute resolution mechanism in place that can be used.

Possible third party dispute resolution programs in the U.S. include those run by businesses such as BBBOnline, TRUSTe, AICPA WebTrust and the Direct Marketing Association. In addition, outside arbitration and mediation service such as JAMS or the American Arbitration Association could also be used. In countries with independent DPAs, the appropriate DPA could provide the dispute resolution mechanism. In other countries, such as Japan, other private dispute resolution mechanisms are available.

The dispute resolution mechanism, to be effective, must be independent, readily available and affordable. Damages, penalties and/or sanctions may be awarded where the applicable law or private sector initiatives so provide. A business should also be obligated to remedy problems arising out of its failure to comply with its Code, and persistent failures of the business to comply with rulings could result in the loss of their Code certification.

If the dispute still cannot be resolved, then the matter would be referred to the applicable governmental or regulatory body responsible for privacy protection (such as the FTC, FCC, OCC, Securities Exchange Commission or other appropriate entity in the U.S.) or, where such an agency does not exist, the public prosecutor in that economy. The governmental or regulatory body would then work with the business and/or third party certification entity (if applicable) to resolve the dispute. If the business refuses to comply with the decision of the regulatory body, then it would also be subject to penalties and sanctions.

VII. Enforcement

As we have seen in the EU context, significant concerns remain about how to make Corporate Privacy Rules "binding" when businesses volunteer to adhere to a set of rules. DPAs in the EU and around the world believe that existing laws do not provide them with the authority

to enforce BCRs or Corporate Privacy Rules. However, even where DPAs lack jurisdiction or do not have the legal means to enforce Corporate Privacy Rules, Corporate Privacy Rules can be legally enforceable and thus "binding" under a number of theories including: revision of corporate bylaws, unilateral declaration, and/or unfair commercial practice laws.

United States

In the United States, for the past ten years, the FTC has used its authority several times under Section 5 of the FTC Act to take action against companies that misrepresent their privacy practices.[80] Corporate Privacy Rules which are included in an on-line privacy policy or some other public statement that is posted on its website (or in the case of workers, on its intranet), could therefore be challenged as unfair or deceptive trade practices where the business fails to comply with its Corporate Privacy Rules.[81]

For example, in 2005, the FTC settled charges against an Internet company that provided shopping cart software to online merchants.[82] According to the FTC, the company rented personal information about merchants' customers to marketers, knowing that such disclosure contradicted merchant privacy policies. The company was barred from disclosing personal information it had previously collected and making future misrepresentations about the collection, use, or disclosure of personally identifiable information. It also required that the company's and merchants' privacy practices be consistent, or, if not, then that company had to disclose in a clear and conspicuous manner that personal information collected on the site would be used, sold, rented, or disclosed to third parties. The settlement also required that the company forfeit monies it made by selling the information and

80. For information on enforcement, see Federal Trade Commission, Enforcement Cases, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited March 23, 2007). For information regarding the FTC's overall investigative and law enforcement authority, see Federal Trade Commission Office of the General Council, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, Sept. 2002, *available at* http://www.ftc.gov/ogc/brfovrvw.htm.

81. Whether the FTC has jurisdiction over issues involving employee data is a matter that has not been settled. To date, the FTC has not taken action against an organization for false or deceptive practices with respect to employee data, and it is an open question whether the FTC can assert such jurisdiction.

82. Agreement Containing Consent Order, Vision I Properties, LLC, File No. 0423068 (Mar. 10, 2005), *available at* http://www.ftc.gov/os/caselist/0423068/050310agree0423068.pdf.

adhere to certain record-keeping provisions that would allow the FTC to monitor compliance with its order.

In 2004, the FTC settled a case against Tower Records involving a security flaw in the company's website that exposed customers' personal information to other Internet users in violation of Tower's privacy policy representations and federal law.[83] Tower Records was barred from making future misrepresentations and was required to implement an appropriate security program and carry out regular outside audits of its website security for the next ten years.

The same year, Gateway Learning Corporation also agreed to settle FTC charges that it violated federal law when it rented consumers' personal information to target marketers.[84] According to the FTC, Gateway Learning rented consumers' information contrary to explicit promises made in its privacy policy and that, after collecting the information, Gateway Learning changed its privacy policy to allow it to share the information with third parties without notifying consumers or obtaining their consent. Gateway Learning was barred from making deceptive claims about how it will use consumers' information and from applying material changes in its privacy policy retroactively without consumers' consent. Gateway Learning was also required to forfeit the money it earned from renting the data.

In 2000, Toysmart.com ("Toysmart") agreed to settle FTC charges that the company misrepresented to consumers that personal information would *never* be shared with third parties and subsequently disclosed, sold or offered that information for sale in direct violation of the company's own privacy statement. The settlement agreement forbade the sale of Toysmart's customer information except under very limited circumstances.[85]

As the actions taken by the FTC over the past decade demonstrate, it is possible to enforce public representations about privacy practices under laws applicable to unfair commercial practices. Many countries around the world have similar laws in place that may enable the DPAs or other relevant authorities to prosecute businesses that fail to adhere to their Corporate Privacy Rules.

Other federal agencies have similar powers. For example the finan-

---

83. Agreement Containing Consent Order, MTS, Inc, File No. 032-3209 (Apr. 21, 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040421agree0323209.pdf.

84. Agreement Containing Consent Order, Gateway Learning Corp., File No. 042-3047 (July 7, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf.

85. FTC v. Toysmart.com, LLC, No. 00-CV-11341, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000).

cial regulators have similar authority under the bank regulatory acts with respect to false and deceptive practices by banks.[86]

European Union

It is also possible to enforce Corporate Privacy Rules in the EU using an approach similar to that found in the U.S., under the theory of "unilateral undertakings" or a public declaration. Unfair trade practices laws, as well as general rules on misrepresentation and misleading advertisement, can in fact provide sufficient legal guarantees.[87] If businesses are obligated to publish Corporate Privacy Rules, as recommended in this article, and if they then fail to follow those rules, businesses could be challenged by national regulators and individuals. In this respect, the 2005 Directive on Unfair Commercial Practices[88] ("Unfair Commercial Practices Directive") harmonizes Member State laws in this area. The purpose of the Unfair Commercial Practices Directive is to protect consumers from unfair commercial practices and businesses from unfair business practices by their competitors. In particular, it introduced individual rights of action in all Member States that will enable individuals to enforce their rights against unfair commercial practices. According to a recently published article by Leonardo Cervera Navas, an official of the EU Commission who worked in the data protection field, a "definitive solution to the problem of the so-called 'external binding effect' of Binding Corporate Privacy Rules appears to be attainable in the EU context."[89]

Cervera argued that the Unfair Commercial Practices Directive provides the enforcement hook sought by the EU data protection community. Cervera argued that anything that impairs the consumer's ability to make an informed decision, and thus causes the consumer to make a decision that he or she might not otherwise make, would

86. *See* 12 U.S.C. § 1818(b) (2006); 15 U.S.C. § 45(a) (2006). *See also* Letter from Alan Greenspan, Chairman, Federal Reserve, to Congressman John LaFalce, Ranking Member, Committee on Financial Services (May 30, 2002), *available at* http://www.federalreserve.gov/boarddocs/press/bcreg/2002/20020530/attachment.pdf.

87. Henning Kahlert: Unlautere Werbung mit Selbstverpflichtung, Wettbewerbsrechtliche Problem emit Datenschutz im Internet, DuD (2003), 412.

88. Parliament and Council Directive (EC) No. 29/2005 of 11 May 2005, 2005 O.J. (L 149) 22, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_149/l_14920050611en00220039.pdf.

89. Leonardo Cervera Navas, *The New Directive on the Unfair Commercial Practices in the Internal Market as a Promising Tool for the Uptake of Binding Corporate Rules*, 20 INT'L REV. L. COMPUTERS & TECH. 343 (2006).

constitute a material distortion of consumers' economic behavior.[90] Moreover, declaring that certain standards of data protection are being applied when that is, in fact, not the case would likely be considered contrary to the requirements of professional diligence and therefore constitute an unfair commercial practice as defined by the Directive.[91] Consequently, Cervera concluded that failure to honor Corporate Privacy Rules commitments would constitute an unfair trade practice.[92] In his view, it is reasonable to think that DPAs can be considered to be competent authorities for exercising the power confirmed by the Directive and hearing claims. Moreover, he suggested that the Directive may increase the enforcement power of some DPAs in certain Member States where enforcement powers are more limited.[93]

In addition, national labor laws are likely to provide redress to employees should the employer make erroneous statements about the processing of personnel data, for example, in the labor contract or on its intranet.

Other Countries

A survey of consumer protection laws in Asia and the Americas has found that many countries in those regions have laws that prohibit false or misleading representation and/or unfair business practices. In Asia, countries such as Australia, India, Indonesia, Japan, Korea, New Zealand, the Philippines, and Thailand have laws in this area that provide individual redress and/or administrative sanctions including fines and injunctions. All of these countries have established enforcement bodies or delegated enforcement to particular executive departments.[94] In

90. *See id.* § 6.2.

91. *Id.*

92. *Id.*

93. *See id.* § 6.4.

94. The following are the respective designated authorities and consumer protection laws: *Australia*—Australian Competition and Consumer Commission, http://www.accc.gov.au/content/index.phtml/itemId/142, and the Trade Practices Act, 1974 (Austl.), *available at* http://www.austlii.edu.au/au/legis/cth/consol_act/tpa1974149/index.html; *India*—National Consumer Disputes Redress Commission, http://ncdrc.nic.in, and the Consumer Protection Act, No. 68 of 1986, *available at* http://ncdrc.nic.in; *Indonesia*—National Consumer Protection Board and the Law on Consumer Protection , No. 8 of 1999; *Japan*—Japanese Cabinet Office, Quality of Life Bureau, http://www.cao.go.jp/index-e.html, and the Consumer Protection Fundamental Act, Law No. 78 of 1968 (as amended), *available at* http://www.apeccp.org.tw/doc/Japan/Comlaw/jpiss01.html; *Korea*—Korea Consumer Protection Board, http://english.cpb.or.kr, and the Consumer Protection Act, Act No. 3921 of 1986 (as amended), *available at* http://english.cpb.or.kr; *New Zealand*—Ministry of Consumer Affairs, http://www.consumeraffairs.govt.nz, Commerce

the Americas, countries such as Mexico, Barbados, Brazil, Chile, Costa Rica, Panama, Paraguay, and Uruguay, have designated authorities and in most cases consumer protections laws that may provide appropriate legal bases on which to enforce Corporate Privacy Rules.[95] Particularly in Central and South America, where few privacy laws have been enacted, these consumer protection laws may provide a promising avenue for enforcement of public promises made by businesses.

More and more countries are adopting or strengthening their unfair commercial practices or consumer protection laws, largely in response to efforts underway at the OECD and the United Nations. Both the U.N. and the OECD have issued guidelines on consumer protection that call for protection against unfair and misleading commercial

---

Commission, http://www.comcom.govt.nz, and the Fair Trading Act , No. 121 of 1986, *available at* http://www.legislation.govt.nz/libraries/contents/om_isapi.dll?clientID=3417260055&infobase=pal_statutes.nfo&jump=a1986-121&softpage=DOC; *Philippines*—Bureau of Trade Regulation and Consumer Protection, Ministry of Commerce, http://www.business.gov.ph/About_Organizational_Chart.php, and Consumer Act, Republic Act No. 7394 of 1991, *available at* http://www.business.gov.ph/uploads/files/Forms1_File_1104836450_RA7394.pdf; and *Thailand*—Consumer Protection Board, http://www.ocpb.go.th, and the Consumer Protection Act, B.E. 2522 (1979).

95. The following are the respective designated authorities and consumer protection laws: *Barbados*—Fair Trading Commission, http://www.ftc.gov.bb, and the Consumer Protection Act, 1 L.R.O. 2002, Cap.326D, *available at* http://www.commerce.gov.bb/Legislation/Documents/Consumer%20Protection%20Act,Cap326D.pdf; *Brazil*—Office of Consumer Protection, Ministry of Justice, http://www.mj.gov.br/DPDC/index.htm, and the Código de Defesa do Consumidor, Law No. 8.078 of Sept. 11, 1990, *available at* http://www.mj.gov.br/DPDC/servicos/legislacao/pdf/cdc.pdf; *Chile*—the National Consumer Service (SERNAC), http://www.sernac.cl, and Ley No. 19.496, *available at* http://www.sernac.cl/docs/texto_ley_del_consumidor.pdf; *Costa Rica*—Directorate of Consumer Support, http://www.meic.go.cr/esp2/consumidor, and Ley No. 7472 de Promoción de la Competencia y Defensa Efectiva del Consumidor [Law No. 7472 on Promotion of the Competition and Consumer Protection], Gaceta 14, Jan. 14, 1995, *available at* http://www.meic.go.cr/esp2/informacion/leypromo.html; *Mexico*—Profecco, http://www.profeco.gob.mx, and the Ley Federal de Protección al Consumidor, DOF Dec. 24, 1992, p. 26, *available at* http://www.diputados.gob.mx/LeyesBiblio/ref/lfpc/LFPC_orig_24dic92_ima.pdf; *Panama*—Authority for Consumer Protection and Competition Defense, http://www.autoridaddelconsumidor.gob.pa, and Ley No. 29 of 1 Feb. 1996, *available at* http://www.autoridaddelconsumidor-.gob.pa/pdf/ley29febrero96.pdf; *Paraguay*—National Integrated Consumer Protection System, http://www.mic.gov.py/snipc, and Ley No. 1334 De Defensa Del Consumidor Y Del Usuario [Law No. 1334 On Consumer and User Protection], *available at* http://www.mic.gov.py/snipc/marco_juridico/Ley_1334.pdf; and *Uruguay*—Ministry of Economy and Finance Office of Defense of Consumer, http://www.defcon.gub.uy, and Ley de Relaciones de Consumo [Law on Consumer Relations], No. 17.250 of 11 August 2000, *available at* http://www.defcon.gub.uy/informacion/index.php?IndexId=56.

practices.[96] Consumer protection laws, however, may not work to regulate public declarations made by businesses relating to personal information of their employees. Using existing unfair competition laws or consumer protection laws as a back stop to enforcing public declarations relating to consumer information could go a long way to creating an enforceable global privacy regime for consumer information without having to wait for new laws to be passed or an international accord to be reached.[97]

VIII. CROSS-BORDER COOPERATION

In addition to having the appropriate legal basis on which to enforce Corporate Privacy Rules, there needs to be a commitment among the respective enforcement authorities to cooperate in the event of cross-border disputes or breaches. Such an agreement could take a form similar to a mutual recognition or cooperation agreement. While such cross-border cooperation and collaboration would not be easy to accomplish, it is not unprecedented. In fact, government agencies around the world are already collaborating closely in such areas as law enforcement, spam, and identity theft. The following are some examples of where such cooperation is already occurring; any of these existing networks could serve as a source or model for cooperation in the privacy area.

Spam. In October 2004, government agencies around the world joined forces to combat spam on a global level with an Action Plan on Spam Enforcement. The Action Plan, endorsed by nineteen agencies from fifteen countries, calls for increased investigative training, the establishment of contact points within each agency to respond quickly and effectively to enforcement inquiries, and the creation of an international working group for spam regulation.[98]

Consumer Protection. The International Consumer Protection and Enforcement Network (ICPEN), formerly known as the International Marketing Supervision Network (IMSN), is a membership business

96. *See* UNDESA, *United Nations Guidelines for Consumer Protection* (2003), http://www.un.org/esa/sustdev/publications/consumption_en.pdf; OECD, *Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce* (2000), http://www.oecd.org/dataoecd/18/13/34023235.pdf .

97. During their 2006 meeting, the International Conference of Data Protection and Privacy Commissioners called for the development of an international privacy convention. The 2006 conference communiqué is available at http://ico.crl.uk.com/files/FinalConf.pdf.

98. *See The London Action Plan on International Spam Enforcement Cooperation* (2004), http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf.

consisting of the trade practice law enforcement authorities of more than two dozen countries.[99] The mandate of the ICPEN is to share information about cross-border commercial activities that may affect consumer interests and to encourage international cooperation among law enforcement agencies.

Consumer Fraud/Identity Theft. Consumer Sentinel members include more than 1000 law enforcement agencies in Australia, Canada, and the United States.[100] It helps them build cases and detect trends in consumer fraud and identity theft. Consumer Sentinel gives law enforcers access to over one million complaints, including consumer complaints from numerous Better Business Bureaus, the National Fraud Information Center and Canada's PhoneBusters.

Anti-trust. The International Competition Network (ICN) provides anti-trust agencies from developed and developing countries with a network for addressing practical anti-trust enforcement and policy issues of common concern.[101]

CONCLUSION

Given the weaknesses in existing approaches to cross-border data transfers, a new truly global solution is needed sooner rather than later. Consumers, business, and countries are being disadvantaged by the existing patchwork of cross-border privacy rules. Countries with strict or complex cross-border restrictions, particularly those in the developing world, are likely to lose out on new business investment and outsourcing opportunities. Moreover, increased regulation does not mean increased privacy protection. To the contrary, the overly complex maze of regulation discourages compliance as well as the provision of products and services. Concern about the lack of business compliance was raised as an issue, for example, in Japan during the government's public consultation on the review of the Personal Information Protection Law.[102]

As we have discussed, the use of Corporate Privacy Rules offers a way

99. Information on the International Consumer Protection and Enforcement Network is available at http://icpen.cpb.or.kr/en.

100. Information on Consumer Sentinel is available at http://www.consumer.gov/sentinel.

101. Information on the International Competition Network is available at http://www.internationalcompetitionnetwork.org.

102. In particular, the discussion document questioned why there were such disparities in how businesses protect personal information and noted that some businesses have stopped providing services such as the public directories because they find the rules to be overly burdensome. *See* Personal Information Protection Committee, Quality of Life Policy Council,

to correct the problems associated with the current patchwork of cross-border privacy rules and provide significant benefits to companies and individuals alike. By enabling companies to implement consistent privacy policies and practices on a global basis, individuals will be afforded more meaningful privacy protections. Their personal information will be protected in a uniform and consistent manner across an organization no matter where the information may be transferred. In addition, because companies would be required to remain accountable for the protection of personal information under their control and address complaints when they arise, individuals would have recourse for the first time in jurisdictions with no privacy laws and, in some cases, more effective recourse in those jurisdictions with existing privacy laws.

Corporate Privacy Rules would also eliminate the need to determine the legal regime applicable to the cross-border data processing activities of the company since the processing would be subject to a single set of privacy principles, rather than the laws of the multiple countries from where the data emanate. In addition, Corporate Privacy Rules can be tailored to the needs of individual companies taking account of particular challenges and sensitivities, the corporate culture, processes and the organizational structure. Corporate Privacy Rules are also easier to administer than contracts and in some cases do not require approval by certain DPAs. In sum, providing companies the freedom to move data globally among affiliates in accordance with their Corporate Privacy Rules can provide important benefits to everyone, including the provision of seamless twenty-four-hour customer service, a wider array of products and services at lower prices, enhanced privacy protections, better and more uniform workforce training and education, and reduced corporate administrative burdens.

Nonetheless, many DPAs continue to call for the development of international data privacy standards or an international privacy convention as the best way to address the disparities in privacy protection around the world.[103] At best, however, this will take years

---

Japanese Cabinet Office, Main Issues for Consideration with Respect to the Protection of Personal Information (discussion paper) (July 28, 2006).

103. The International Conference of Data Protection and Privacy Commissioners has repeatedly called for the development of international data privacy standards since 2003 and, most recently, in 2006 for the establishment of an international privacy convention. *See* Data Protection and Privacy Commissioners 2003, Commissioner Resolutions, http://www.privacyconference2003.org/commissioners.asp; Press Release, Swiss Federal Data Protection

to accomplish, presuming that agreement can be reached within the international community to develop such a convention. Even if such a convention is agreed upon, several additional years will be required for countries to conform their national laws to the convention.

The attractiveness of Corporate Privacy Rules is that they can be implemented without, in most instances, enacting new laws or regulations. The challenge will be for governments to devote the necessary time and effort to:

- Identify existing means within national law to enforce Corporate Privacy Rules, such as through consumer protection, unfair trade practices, and/or privacy laws;
- Establish a national approach to verification and approval of Corporate Privacy Rules; and
- Establish a cross-border cooperation mechanism and a system for mutual recognition or acceptance of Corporate Privacy Rules.

These tasks, however, are eminently achievable. In any case, whatever global solution is ultimately agreed upon, it is clear that it has to greatly simplify the current arrangement. Once a practical global solution is developed, compliance will increase, thus increasing privacy protection for everyone concerned, and greater economic benefits will flow to countries that permit businesses to utilize a global solution for their cross-border data transfers.

While some companies are experimenting with the EU approach to BCRs, that approach is not likely to be widely embraced by global businesses because it seeks to apply EU standards on a global basis. In particular, it applies standards that are equivalent to or supersede those that a European company must abide by. For example, the EU approach to BCRs requires an entity established in the EU to be the guarantor for the entire global corporate family.[104]

Attainment of a global solution is within reach if governments show sufficient flexibility and strive for comparable rather than equivalent

---

and Information Commissioner, 27th International Conference of Data Protection and Privacy Commissioners, Montreux (14-16 September 2005) Towards the Recognition of a Universal Right to Data Protection and Privacy (Sept. 16, 2005), http://www.edoeb.admin.ch/dokumentation/00438/00465/00888/00893/index.html?lang=en; 28th International Conference of Data Protection and Privacy Commissioners, Closing Communiqué, http://ico.crl.uk.com/files/FinalConf.pdf.

104. *See* Karin Retzer, *Land in Sight: The Latest Developments Concerning Data Transfers from the EU*, http://www.mofo.com/news/updates/files/update1428.html.

protection. Moreover, a strong commitment to finding a common solution and creative "can do" thinking will be needed. Individuals, businesses and governments all have a stake in resolving this issue so that individuals can have meaningful protections for their personal information as well as access to a wide variety of products and services at competitive prices.